

# Security Enhancement and Eminent Verification Measures of Global Distinctive E-Passport

Dr. R. Mohana Priya, V. Bharanitharan, S. Clementinbaraj, R. Kirubaharan

Department of Electronics and Communication Engineering,  
Paavai Engineering College, Pachal, Tamil Nadu, India

## ABSTRACT

Electronic Passport is one of the results of the electronic revolution in The World; since the passport is the document of the person in terms of identity and nationality and is the property of the country. One of the most important Challenges is to protect this document from forgery. The common forgery for the Passport is replacing its holder photo. The proposed system concentrates on the Security part of the e-passport. It consists of two parts; the first part is hiding of the security code by using steganography and storing the same code in the issuing Country of the e-passport. The other part will be operated at the control point of the destination country to make sure of the e-passport validity by checking the Hidden code using NFC and verify it with the one. If the two values are equal, then the system will compute a key using Diffie-Hellman Key Exchange. This Key will be used to read the secret information. The project designed is an Authentication system where the Passport holder is authorized through Technology. Electronic passports include contactless chip which stores personal Data of the passport holder, information about the passport and the issuing Institution. In its simplest form an electronic passport contains just a collection of Read-only files, more advanced variants can include sophisticated cryptographic Mechanisms protecting security of the document and / or privacy of the passport Holder.

**KEYWORDS:** ASP- Application Service Provider, BAC- Basic Access Control, IACCO -International Civil Aviation Organization , LCD- Liquid Crystal Display, PKI- Public Key Information, PLC -Programmable Logic Controller, RFID -Radio Frequency Identification, UID -Unique Identification Number, VAL -Ventilator Associated Pneumonia, VAW -Visa Waiver Program

## INTRODUCTION

The project designed is AN authentication system wherever the passport holder is permissible through RFID technology. The passport holder would have AN RFID tag that contains all the passport details like name, number, position etc. This tag must be swiped ridiculous and hence the data subsequently read is given to a microcontroller of 8051 family. This data is matched with the one hold on among the microcontroller, if the data matches microcontroller displays associate degree confirmation message otherwise displays a denial message on an alphanumeric display screen. The status of a specific person also can be obtained through a standing button within the system. Passport verification and checking may be a very time consuming process. This proposed system simplifies the method by giving the authorized person an RFID tag containing all the passport details like name, passport number and nationality etc. Once, the person places the cardboard ahead of the RFID card reader, it reads the info and verifies it thereupon data present within the system and if it matches then it displays the small print of the passport holder. Here we use microcontroller from 8051 family. For display a 16X2 LCD is used.

The status can also be retrieved from this technique by pressing the status button interfaced to a microcontroller. An electronic passport (ePassport) is associate ID document

that possesses connected biographical or biometric data of its bearer. It is embedded in Radio Frequency Identification chip (RFID Tag) which is accomplished of cryptographic functionality. The successful implementation of biometric techniques in documents such as E-Passports aims to the strength of border. Security by decreasing the chance of copy or pretend passport and making while not hesitation of identity of the documents' holder. The e-Passport additionally offers substantial advantages to the rightful holder by providing a lot of refined means that of confirming that the passport belongs thereto person which it's authentic, without jeopardizing privacy. The states are currently issuing e Passports, which corresponds to more than 50% of all passports being issued worldwide. This represents a good sweetening in national and international security because it improves the integrity of passports by the necessity to match the data contained within the chip.

## LITERATURE REVIEW:

Thus, the data stored in this card is referred as the passport details of the person. The system architecture of the research work .In these details of the person would be fed into the microcontroller and a unique number is allocated to the person that number is printed Of RFID tag. The RFID reader reads the details of the RFID passport and sends the data to Controller with the help of RF reader. Here, the controllers

**How to cite this paper:** Dr. R. Mohana Priya | V. Bharanitharan | S. Clementinbaraj | R. Kirubaharan "Security Enhancement and Eminent Verification Measures of Global Distinctive E-Passport" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-3, April 2021, pp.1017-1021, URL: [www.ijtsrd.com/papers/ijtsrd41101.pdf](http://www.ijtsrd.com/papers/ijtsrd41101.pdf)



IJTSRD41101

Copyright © 2021 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (<http://creativecommons.org/licenses/by/4.0>)



compares with the data already there. If it matches then the person is allowed to pass gate1 motor 1 is The LCD displays give the guidance to the person to scan the finger. The fingerprint sensor is used to for Biometric verification of the person. The main functionality of this project is to access the passport details of a Passport holder through RFID technology. For this purpose the authorized person is given An RFID card. This card contains an integrated circuit that is used for storing, processing Information through modulating and demodulating of the radio frequency signal that is being transmitted. Thus, the data stored in this card is referred as the passport details of the person. The system architecture of the research work is shown in fig. In this the details of the person would be fed into the microcontroller and a unique number is allocated to the person that Number is printed of RFID tag. The RFID reader reads the details of the RFID passport and Sends the data to controller with the help of RF reader. Here, the controllers compares with the data already there. If it matches then the person is allowed to pass gate1 (motor 1 is The LCD displays give the guidance to the person to scan the finger. The fingerprint sensor is used to for biometric verification of the person. When the fingerprint is scanned it is compare to with the fingerprint stored in the controller to the respective card). RFID technology can be used in form of barcode and embedded chip.

RFID system consists of three components namely transponder (tag), Interrogator (reader) and computer containing the database. The interrogator reads the tag Data and transmits it to the computer for authentication. The information is processed and upon verification, access is granted. The system offers diverse frequency band ranging from Low frequencies to microwave frequencies [5]: Low Frequency: 125-134 KHz High Frequency: 13.56 MHz Ultra High Frequency: 902-928 MHz Microwave Frequency: 2.4 GHz depending upon the source of electrical energy, RFID tags are classified as either Active or passive. The active tags use a battery for powering the circuit on the tag and transmit the tag information upon the reader request. However, these tags are very expensive and seldom used. On the other hands, passive tags get energy from the reader to power their Circuit. These tags are very cost-effective and hence most of the applications use them. A Comparison of these tags highlighting important features. In the present work, passive RFID Tags have been used. A passive RFID tag transmits information to the reader when it comes In the vicinity of electromagnetic field generated by the reader. The computer system uses face recognition algorithm to verify the user. If a Match is found, computer system asks the exit controller to grant permission to the user to leave the hostel. After the user has left the hostel, exit controller sends a request to the Entrance controller through main controller to update the user entrance status. In case of nonregistered user, heavy fine is included in hostel dues of the user for using the card of other Person. The exit monitoring controller thus enables the system to allow the valid person to leave the hostel.

A reader device at the gate reads this data from the vehicle and compares it with the data in the computer database. Information retrieval from Server: In this server the Vehicle number, owners name, registration number and other personal details this would be Retrieved while vehicle crosses the toll gate reader Automatic Transaction details updating: The corresponding amount for each vehicle would be transacted automatically when the Vehicle passes away

the toll gate In Toll gate section we also additional features as theft Detection. If any vehicles are stolen we can easily dated it using the RFID provided to each Vehicle which is a unique one. In the existing system in tollgate section every thing we have to do manually. So it will take time. Because of this traffic jam problems also will occurs. This is in line with the developed countries like USA, England, German and Japan, where RFID, GPS and GSM technologies are widely used for traffic management. Verified by the Security and the vehicle gets the relevant receipt, if the details are verified after the Transaction then goes to actuator unit and then the gate opens automatically

### PROPOSED EXPLANATIONS:

The project designed is an authentication system where the passport holder is authorized through RFID technology. The passport holder would have an RFID tag which contains all the passport details like name, number, nationality etc. This tag has to be swiped over the reader and the information thus read is provided to a microcontroller of 8051 family. This information is matched with the one stored in the microcontroller, if the data matches Microcontroller displays an confirmation message otherwise displays a denial message on a LCD screen. The status of a particular person can also be obtained through a status button in the system. Passport verification and checking is a very time consuming process. This Proposed system simplifies the process by giving the authorized person an RFID tag containing all the passport details like name, passport number and nationality etc. Once, the Person places the card in front of the RFID card reader, it reads the data and verifies it with that data present in the system and if it matches then it displays the details of the passport Holder. Here we use microcontroller from 8051 family.

An electronic passport (ePassport) is an ID document which possesses related Biographic or biometric information of its bearer. It is embedded in Radio Frequency Identification chip (RFID Tag) which is accomplished of cryptographic functionality. The Successful implementation of biometric techniques in documents such as E-Passports aims to the strength of border security by decreasing the possibility of copy or fake passport and Creating without hesitation of identity of the documents' holder. The e-Passport also offers Substantial benefits to the rightful holder by providing a more sophisticated means of Confirming that the passport belongs to that person and that it is authentic, without Jeopardizing privacy. The states are currently issuing ePassports, which corresponds to more Than 50% of all passports being issued worldwide. This represents a great enhancement in National and international security as it improves the integrity of passports by the need to Match the information contained in the chip to the one printed in the document and to the Physical characteristics of the holders; and enables machine-assisted verification of Biometric and biographic information to confirm the identity of travellers Electronic passport There is an international standard ICAO. ICAO stands for International Civil Aviation Organization. The ICAO provides boundary security standards or set of rules. Each country follows this standard but the verification method may differ for different countries.

### FINGER PRINT SENSORS:

Fingerprint sensing techniques can be of two types – off-line scanning and live scanning. In off-line sensing fingerprints are obtained on paper by “ink technique” which are then scanned using paper scanners to produce the digital image.

Most AFISs use live scanning where the prints are directly obtained using an electronic fingerprint scanner. Almost all the existing sensors belong to one of the three families: optical, solid-state, and Ultrasound. Optical sensors, based on the frustrated total internal reflection (FTIR) technique are commonly used to capture live-scan fingerprints in forensic and government Applications. They are the most common fingerprint sensors. Solid-state touch and sweep Sensors — silicon-based devices that measure the differences in physical properties such as Capacitance or conductance of the friction ridges and valleys dominate in commercial Applications. Tartagni and Guerrieri describe a feedback capacitive sensing scheme using a 200x200 element sensor array implement in standard 2-metal CMOS technology. JeongWoo Lee et al [20] discuss another such solid-state sensor, based on capacitive differences, Capable of producing 600dpi fingerprints. Many commercially available sweep sensors like Fujitsu MBF320 are based on such low-power solid-state devices. A special case of off-line sensing is the acquisition of a latent fingerprint from a Crime scene. Used extensively in forensics, latent prints are accidental impressions left by Friction ridge skin on a surface, due to natural secretions of the eccrine glands present o Skin. While tremendous progress has been made in plain fingerprint matching, latent Fingerprint matching continues to be a difficult problem. Poor quality of ridge impressions, Small finger area, and large non-linear distortion are the main difficulties in latent fingerprint Matching, compared to plain fingerprint matching. For the purpose of automation, a suitable Representation i.e. feature extraction of fingerprints is essential. This representation should have the following properties

#### FACE RECOGNITION SENSORS:

Real time face recognition is part of the field of biometrics. Biometrics is the ability for a computer to recognize a human through a unique physical trait. Face recognition provides the Capability for the computer to recognize a human by facial Characteristics. Today, biometrics is one of the fastest growing Fields in advanced technology. Predictions indicate a Biometrics explosion in the next century, to authenticate Identities and avoid and unauthorized access to networks, Database and facilities. A facial recognition device is a device that takes an image or a video of a human face and compares it to other image Faces in a database. The structure, shape and proportions of the Faces are compared during the face recognition steps. In Addition, distance between the eyes, nose, mouth and jaw, Upper outlines of the eye sockets, the sides of the mouth, Location of the nose and eyes, and the area surrounding the Check bones are also compare When using a facial recognition program, several pictures Of the person must be taken at different angles and with Different facial expressions [1]. At time of verification and Identification the subject stands in front of the camera for a few Seconds, and then the image is compared to those that have been previously recorded. Facial recognition is widely used because of its benefits. The advantages of facial recognition are that it is not intrusive, Can be done from a faraway distance even without the person Being aware that he/she is being scanned. Such thing is Needed in banks or government offices for example, and this is What makes facial recognition systems better than other Biometric techniques in that they can be used for surveillance Purposes like searching for wanted criminals, suspected Terrorists, or missing children. Face recognition devices are most beneficial to use for Facial authentication than for

identification purposes, because it is easy to alter someone's face, and because the person can disguise using a mask. Environment is also a consideration as Well as subject motion and focus on the camera Facial recognition, when used in combination with another Biometric method, can improve verification and identification Results dramatically.

#### ARDUINO UNO:

The Arduino Uno has a number of facilities for communicating with a computer, another Arduino, or other Microcontrollers. The ATmega328 provides UART TTL (5V) serial communication, which is available on Digital pins 0 (RX) and 1 (TX). An ATmega8U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer. The '8U2 firmware uses the standard USB COM drivers, and no external driver is needed. However, on Windows, an \*.inf file is required. The Arduino software includes a serial monitor which allows simple textual data to be sent to and from the Arduino board. The RX and TX LEDs on the board will flash when data is being transmitted via the USB-to serial chip and USB connection to the computer (but not for serial communication on pins Rather than requiring a physical press of the reset button before an upload, the Arduino Uno is designed in a Way that allows it to be reset by software running on a connected computer. One of the hardware flow control Lines (DTR) of the ATmega8U2 is connected to the reset line of the ATmega328 via a 100 nanofarad Capacitor. When this line is asserted (taken low), the reset line drops long enough to reset the chip. The Arduino software uses this capability to allow you to upload code by simply pressing the upload button in the Arduino environment. This means that the bootloader can have a shorter timeout, as the lowering of DTR Can be well-coordinated with the start of the upload. This setup has other implications. When the Uno is connected to either a computer running Mac OS X or Linux, it resets each time a connection is made to it from software (via USB). For the following half-second or so, the bootloader is running on the Uno. While it is programmed to ignore malformed data (i.e. anything besides an upload of new code), it will intercept the first few bytes of data sent to the board after a Connection is opened. If a sketch running on the board receives one-time configuration or other data when it first starts, make sure that the software with which it communicates waits a second after opening Connection and before sending this data. The Uno contains a trace that can be cut to disable the auto-reset. The pads on either side of the trace can be soldered together to re-enable it. It's labelled "RESET-EN". You may also be able to disable the auto-reset by connecting a 110 ohm resistor from 5V to the reset line.

#### RFID TAG:

This section describes out of which parts RFID tags consist of, how they work in principle, and what types of Tags do exist. It focuses on how tags are powered and what frequency ranges is used. The section concludes By covering a few important standards. The size of the chip depends mostly on the Antenna. Its size and form is dependent on the frequency the tag is using. The size of a tag also depends on its area of use. It can range from less than a millimetre for implants to the size of a book in container logistic. In addition to the micro chip, some tags also have rewritable memory Attached where the tag can store updates between reading cycles or new data like serial numbers. A RFID tag is shown in figure 1. The antenna is clearly visible. As said



before the antenna has the largest Impact of the size of the tag. The microchip is visible in the center of the tag, and since this is a passive tag it does not have an internal power source. In principle an RFID tag works as follows: the reading unit generates an electro-magnetic field which induces a current into the tag's antenna. The current is used to power the chip. In passive tags the current also charges a condenser which assures uninterrupted power for the chip. In active tags a battery replaces the condenser. The difference between active and passive tags is explained shortly. Once activated the tag receives Commands from the reading unit and replies by sending its serial number or the requested information. II General the tag does not have enough energy to create its own electro-magnetic field, instead it uses back Scattering to modulate (reflect/absorb) the field sent by the reading unit. Because most fluids absorb electromagnetic fields and most metal reflect those fields the reading of tags in presence of those materials is Complicated. During a reading cycle, the reader has to continuously power the tag. The created field is called continuous Wave, and because the strength of the field decreases with the square of the distance the readers have to use on Rather large power. That field overpowers any response a tag could give, so therefore tags reply on Side-channels which are located directly below and above the frequency of the continuous wave

#### CONCLUSION:

The process in science and technology is a non stop process. New things and new technology are being invented. As the technology grows day by day, we can imagine about the future in which things we may occupy every place. The proposed system based on Arduino Uno is found to be more compact, user- friendly and less Complex, which can be really be used in order to perform. Several tedious and repetitive tasks. Through it is designed keeping in mind about the need for necessary industry; it can extend for other purpose such as commercial and research application. Due to probability of high technology Arduino Uno and RFID tag used this advanced safety system passport and finger print sensors for "SECURITY ENHANCEMENT AND EMINENT VERIFICATION MEASURE OF GLOBAL DISTINCTIVE E-PASSPORT" it fully Hardware control with less software circuit. The feature make this system is base for future system the principle of the development of science is that "nothing is impossible" so we shall look forward to your bright and sophisticated world.

#### REFERENCE:

- [1] G. Mathew Ezovski, & Steve E. Watkins, The Electronic Passport and The Future of Govt. Issued RFID based identification||, IEEE International Conference on RFID, 28 March 2007. V. K. Narendira Kumar & Dr. B. Srinivasan, Biometric Passport Validation Scheme using Radio Frequency Identification||, I. J. Computer Network and Information Security, April 2013.
- [2] D. L. Wu, Wing W. Y. NG, D. S. Yeung, and H. L. Ding, —A brsurvey On current RFID applications, || in Proc. International Conference on Learning and Cybernatics, Baoding, July 12-15, 2009, pp. 2330-2334 .
- [3] B. Yan and D. Y. lee Design of spot ticket management system based on RFID|| in Proc. International Conference on Network security, Wireless Communications and Trusted Computing, 2009, pp. 496-499.
- [4] M. Arapinis, T. Chothia, E. Ritter, and M. Ryan, Untraceability in the Applied pi calculus, || in proceedings of the 1<sup>st</sup> Int. Workshop on RFID Security and Cryptography. , 2009, to appear.
- [5] K. Nohl and D. Evans, Privacy through noise: a design space for private Identification, || in Annual Computer Security Applications Conference (ACSAC 2009), Marci Meingast, Jennifer King, and Deirdre K. Mulligan, —Security and Privacy Risks of Embedded RFID in Everyday Things: the e-Passport and Beyond, " Journal of Communications.
- [6] Piotr Porwik, "The Biometric Passport: The Technical Requirements and Possibilities of Using", Biometrics and Kansei Engineering, International Conference ICBAKE on 2009, pp. 65
- [7] Dr. Albert B. Jeng, Elizabeth Hsu, And Chia Hung Lin Sponsor: "Should and How cc be used to evaluate RFID based passport, National Communications Commission, Available.
- [8] <https://www.commoncriteriaportal.org/icc/9iccc/pdf/C2404.pdf>
- [9] K. Nohl and D. Evans, Privacy through noise: a design space for private Identification, in Annual Computer Security Applications Conference (A. CSAC 2009), 2009.
- [10] Piotr Porwik, "The Biometric Passport: The Technical Requirements and Possibilities of Using", Biometrics and Kansei Engineering, International Conference ICABAKE on 2009, pp. 65
- [1] G. Mathew Ezovski, & Steve E. Watkins, The Electronic Passport and The Future of Govt. Issued RFID based

